(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 April 2002 (25.04.2002)

PCT

(10) International Publication Number
WO 02/32308 A1

(51) International Patent Classification[7]: A61B 5/117, G06F 1/00, H04B 1/00

(21) International Application Number: PCT/SG00/00177

(22) International Filing Date: 17 October 2000 (17.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **KENT RIDGE DIGITAL LABS** [SG/SG]; 21, Heng Mui Keng Terrace, Singapore 119613 (SG).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HUANG, Weimin** [CN/SG]; Block 702, #11-371, West Coast Road, Singapore 120702 (SG). **WU, Jiankang** [CN/SG]; Block 51 #06-565, Teban Gardens Road, Singapore 600051 (SG). **LAM, Chian, Prong** [SG/SG]; 171, Countryside Road, Singapore 786894 (SG).

(74) Agent: **HELEN YEO & PARTNERS**; #33-00 UOB Plaza 1, 80 Raffles Place, Singapore 786894 (SG).

(81) Designated States *(national)*: SG, US.

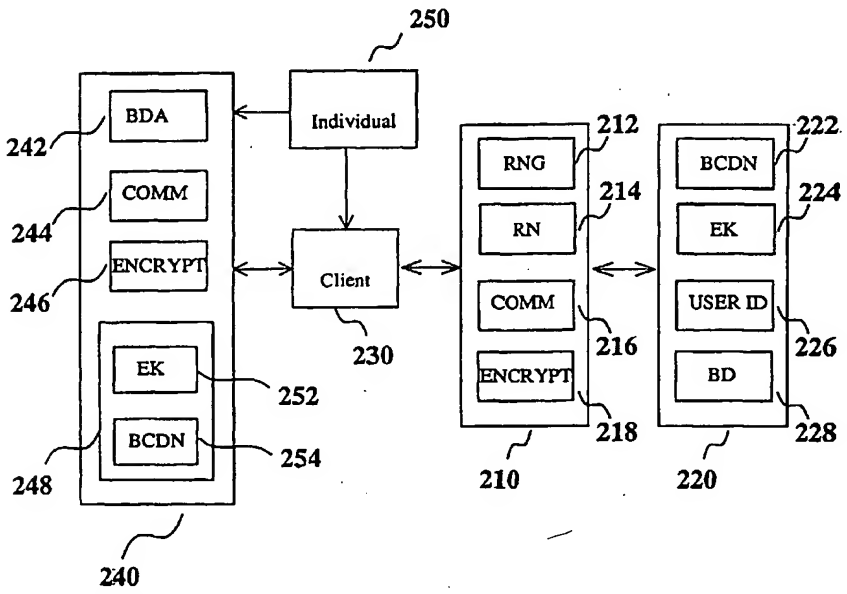
Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: BIOMETRICS AUTHENTICATION SYSTEM AND METHOD



(57) Abstract: A method of identifying redundant email messages and removing the redundant messages from a user's message file. More particularly, to identify redundant messages, there is described a method of copying messages stored in a message file into two different arrays and cleansing one of the arrays so as to remove formatting and header information. These cleansed messages may then be compared to determine whether a particular message is wholly repeated in any other. Messages that are found to be repeated are removed from the other array. The messages remaining in the other array may then be substituted for the messages in the user's message file, resulting in a minimized message file. The method may also be applied to newsgroup postings.

WO 02/32308 A1

BIOMETRICS AUTHENTICATION SYSTEM AND METHOD

TECHNICAL FIELD OF THE INVENTION

The invention relates to a system and method for restricting physical and/or logical access, and more particularly to a secure system and method for authenticating biometric data which prevents authentication of biometric data captured outside the system and reuse of biometric data captured within the system after a single authentication attempt.

BACKGROUND OF THE INVENTION

A typical system according to the prior art using biometric data to control physical or logical access may be described with reference to **FIG. 1**. First, biometric data corresponding to an individual **150** is captured on-line, on a biometric data capture device **140** connected to a client **130**, and then sent to an authentication server **110** together with auxiliary data, for example the customer's birthday, address, banking account information, etc. Upon receiving the biometric data, the server compares the received biometric data against biometric data previously stored in the database **120**. If the received biometric data match stored biometric data, then the server authenticates the individual, who thereby gains access to the information or location guarded by the system.

In such a system, there can be several security holes: First, the network connection between the client and server, if any, may not be secure. There is a need for a secure link between the client and server to prevent access to these communications by unauthorized persons. Second, the client itself must be very secure. Otherwise, someone may use biometric data captured previously or elsewhere for authentication. Third, the capturing device may be susceptible to tampering, and the link between the capturing device and client is vulnerable.

A number of prior art systems and methods have been proposed for controlling physical access to restricted locations and logical access to restricted information.

U.S. Patent No. 5,933,625 discloses a unique time generating device incorporated in a computer and a device allowing sequentially manufactured computers incorporating such a unique time generating device to authenticate each other over a network. Each unique time generating device accumulates elapsed time in unit increments from a starting point which is different for each time generating device, where the starting point assigned to each unique time

device is different by a predetermined interval. Using this device, mutual authentication can be achieved on the basis of the accumulated time by each computer. The unique time data can also be used as a single-use password. The identification and authentication of a computer or a device is based upon the presence and function of the unique time generating device. Therefore, the security of the system is based on the security of the computer. Anyone who acquires a computer containing such a unique time generating device can perform the authorized actions. Such computer authentication cannot be confused with personal authentication. Moreover, U.S. Patent No. 5,933,625 does not concern use of biometric data for personal authentication.

It is known in the prior art to authenticate a user by means of an article the user has in his or her possession, for example an access card, or by means of information known to the user, for example a personal identification number (PIN), for access to buildings, bank accounts and network computer accounts. Such authentication methods are usually used either in a secure or closed environment for example the existing bank automatic teller machine (ATM) system, or for access to locations or information that do not require high security.

Canada Patent No. 1,149,484 discloses a method and apparatus for securing data transmissions. According to the disclosure, a user's PIN and a random number generated at the client are encrypted to form a user identifier code which is transmitted along with the random number to a server for comparison. At the server, a previously stored PIN is accessed from a data file. By applying the same encryption algorithm to the previously stored PIN and the random number transferred from the client, the server generates a new user identifier code, which it compares to that received from the client. A match indicates an authorized user. In another embodiment, a dynamic identifier code, dependent on the random number generated by the client, is used to obviate the need for transferring the PIN to the server. Here, the user PIN may be forgotten, stolen, damaged or lost. In such a case, a fraudulent user identifier code can be generated.

Another method for achieving secure transmission of information is the use of a one-time encryption key (session key), as disclosed in Canada Patent Nos. 1,340,092 and 2,236,406.

Canada Patent No. 2,105,404 (U.S. Patent No. 5,280,527) uses biometric information as part of the "seed" for generating a token, with other information such as time-varying information (*e.g.* the time of day) or a fixed code (*e.g.* PIN). The token is then communicated to

a host system or access device to determine whether access to the host is permitted. The host must be synchronized with the security mechanism so that the time varying code is identical.

U.S. Patent No. 5,343,529 uses a server-generated request identifier that is specific to each transaction to ensure that access information is different for each transaction. The server sends the request identifier to the client requesting access and retrieves a user identifier from a database. By applying the same irreversible transformation to the user identifier and request identifier, authentication code generators at the client and at the server independently generate an authentication code. If the server and client authentication codes match, the server permits access. However, if the user identifier is obtained by someone other than the corresponding user, fraudulent access can be gained. Moreover, such a method cannot be used in an authentication system based on verification of biometric data because the irreversible transformation will not generate the same code for different biometric data samples, as explained in the following: The irreversible transformation is applied to bit strings of the biometric data. If the bit strings are different, the irreversible transform results will also be different. Biometrics samples, even for a single personal characteristic, for example a fingerprint, cannot be exactly the same due to the existence of capturing noise and variations in capturing conditions. Therefore, an irreversible transformation will result in the generation of different codes. Examples of irreversible transforms include the hash algorithm and certain encryption algorithms, in which use of a different key gives a different encryption result.

U.S. Patent No. 5,778,071 discloses a portable security device that can authenticate the individual who carries it and encrypt data communications. This disclosure uses an idea similar to that of Canada Patent No. 1,149,484, which generates a time-varying number and encrypts it together with the user's PIN. The encryption result and the time-varying number are sent to server. At the server end, the user's PIN is retrieved from a database and encrypted together with the received time-varying number to obtain a second encryption result. The user is considered to be authenticated properly if the two encryption results match.

U.S. Patent No. 5,870,723 provides a token-less biometric commercial transaction authorization method and system. It uses a message sequence number, incremented each time a message is sent from a biometric input apparatus (BIA), to indicate each separate attempt to use the device. It also uses a transmission code comprising a hardware identification code together

with the incrementing sequence number to identify the sending BIA and to detect resubmission attacks. The system disclosed in this reference is not readily adapted to use as a multi-purpose device.

None of the prior art mentioned above addresses the security problems listed previously to which prior art systems such as that shown in **FIG. 1** are susceptible.

SUMMARY OF THE INVENTION

The present invention presents a solution to the security holes inherent in prior art systems and methods of user authentication.

The present invention includes a system and method of authenticating biometric data. An embodiment of the method according to the present invention comprises encrypting a first session key with a first encryption key (EK), receiving and decrypting the first session key using a second EK, capturing biometric data (BD) corresponding to a user, encrypting the captured BD using a second session key, receiving and decrypting the encrypted captured BD using the first session key, comparing the captured BD and previously stored BD and verifying that an elapsed time between transmission of the first session key and transmission of the encrypted captured BD does not violate a timeout criterion, so as to authenticate the captured BD, and destroying the first session key.

Another embodiment of the method according to the present invention comprises encrypting a first message identification code (MIC) with a first encryption key, receiving and decrypting the first MIC using a second encryption key, capturing BD corresponding to a user, encrypting the captured BD and a second MIC using the second encryption key, receiving and decrypting the encrypted captured BD and second MIC using the first encryption key, comparing the captured BD and previously stored BD, comparing the second MIC and the first MIC, and verifying that an elapsed time between transmission of the first MIC and transmission of the encrypted captured BD does not violate a timeout criterion, so as to authenticate the captured BD, and destroying the first MIC.

Another embodiment of the method according to the present invention comprises encrypting a first MIC with a first at least a portion of a first encryption key, receiving and decrypting the first MIC using a second at least a portion of the first encryption key, capturing

BD corresponding to a user, encrypting the captured BD and a second MIC using a first at least a portion of a second encryption key, receiving and decrypting the encrypted captured BD and second MIC using a second at least a portion of the second encryption key, comparing the captured BD and previously stored BD, comparing the second MIC and the first MIC, and verifying that an elapsed time between transmission of the first MIC and transmission of the encrypted captured BD does not violate a timeout criterion, so as to authenticate the captured BD, and destroying the first MIC.

An embodiment of a system for authenticating biometric data according to the present invention comprises a secure server, a database connected to the server for storing first biometric data corresponding to a unique user identification code (ID), a client connected to the server, and a biometric data capture device (BCD) connected to the client for capturing second biometric data from a user, wherein the BCD consists of an integrated hardware unit.

In an aspect of the embodiment, a biometric data capture device serial number (BCDN) and a shared symmetric key or a private key associated with the BCD are stored in a memory internal to the BCD and can be read by an encryption module internal to the BCD and authorized personnel but cannot be modified by external intervention.

In a further aspect of the embodiment, the BCDN and shared symmetric key or private key are destroyed by overwriting the locations in memory in which they are stored when an unauthorized user opens the BCD.

The present invention also includes a system and method of verifying live capture of biometric data. An embodiment of the method of verifying live capture of biometric data according to the present invention comprises capturing a sequence of characteristic feature inputs by a user, extracting from the sequence a time-varying property of the characteristic feature inputs wherein said time-varying property is known to evolve in a predictable manner, and comparing the evolution of the time-varying property against a predictive model. The system of verifying live capture of biometric data according to the present invention comprises a biometric sensor for capturing a characteristic feature of a user, a sensor driver for acquiring biometric data corresponding to the user and means for verifying live capture of the biometric data.

The present invention also includes a method of preventing re-use of captured biometric data. An embodiment of the method comprises generating a first session key, using the first

session key to decrypt encrypted captured biometric data, and destroying the first session key.

A further embodiment of the method comprises generating a first message identification code, decrypting encrypted captured biometric data and a second message identification code, and destroying the first message identification code.

The present invention further includes a method of registering a BCD and a method of registering a user of an authentication system. An embodiment of the method of registering a BCD according to the present invention comprises assigning an encryption key to the BCD, writing a first at least a portion of the encryption key and a BCDN corresponding to the BCD into a database, and writing a second at least a portion of the encryption key and BCDN into a memory internal to the BCD.

An embodiment of the method of registering a BCD according to the present invention comprises assigning an ID to the user, capturing live biometric data for the user, storing the biometric data and associated ID in a database, and defining a list of applications to which the user is authorized access.

These and other embodiments of the invention will become readily apparent to those of ordinary skill in the art from the following description of the invention, which is to be read in conjunction with the accompanying drawings and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be better understood with reference to the drawings, in which:

FIG. 1 shows an authentication system typical of the prior art.

FIG. 2 shows an authentication system according to the invention.

FIG. 3 shows an example of an authentication method according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

The invention generally concerns a secure user authentication system and method based on verification of biometric information unique to the user for restricting physical access to locations and/or logical access to information, wherein potential fraudulent use of the system is thwarted by preventing the biometric information from being used more than once. The system

includes a tamper resistant biometric data capture device which may further include a module which verifies that only biometric data captured live may be used to authenticate a user seeking physical or logical access. The invention is a secure solution to the security holes inherent in prior art systems and methods of user authentication.

An example of a user authentication system according to the present invention is shown in FIG. 2. The system comprises a secure server 210, a database 220 connected to the server, a client 230 connected to the server, and a biometric data capture device (BCD) 240 connected to the client. The server 210 controls access to a location, for example a building or safe ("physical access") or to information, for example a bank or computer account or a computer file ("logical access"). The server itself is made secure by safeguarding it by some physical means, for example placing it in a location to which access is strictly limited, and/or digital means, for example a digital firewall. Other methods of securing the server will be evident to those skilled in the art. The server comprises a random number generator 212 for generating a request number (RN) 214 which serves as a session key or a current message identification code, a communication module 216, comprising communication hardware, for example a modem, and associated software, for example a modem driver, an encryption module 218 which performs encryption and decryption functions, and a server memory (not shown). The encryption and decryption algorithms executed by the encryption module are well known in the art and may be resident on one or more application specific integrated circuits (ASIC). Many suitable encryption algorithms are known in the art and are within the scope of the invention, for example International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES), Rivest-Shamir-Adelman Encryption Algorithm (RSA), and elliptic curve cryptosystems (ECC).

The server database stores information relevant to the authentication process, for example a BCD serial number (BCDN) 222 unique to each BCD, an encryption key (EK) 224 corresponding to each BCD, a user identification code (ID) 226 unique to each user, and biometric data (BD) 228 corresponding to each ID, previously captured by a BCD. The EK may take the form of any number of encryption keys known in the art, for example a shared symmetric key or a public key pair comprising a public key and corresponding private key. As is known in the art, in the public key infrastructure system, the public key of a public key pair is assumed to be accessible to all, while access to the corresponding private key is restricted, and there is a trusted third party which issues a public key certificate indicating the entity (*e.g.*

device) to which the public key belongs. In the case of a shared symmetric key, the EK is shared by both the server and the BCD. In the case of a public key pair, the server stores its own private key and a public key corresponding to the BCD's private key, while the BCD stores its own private key and a public key corresponding to the server's private key. The database may be resident as data on a memory device internal to the server or as a data file on a peripheral memory device, for example a disk drive, CD-ROM, etc. The user identification code may be a string of numeric or alphanumeric characters.

The client **230** is an interface between the server and the BCD, allowing data, for example an ID, BCDN, or request for authentication, to be input into the system by a user **250**. The client also allows the transmission of encrypted messages back and forth between the server and the BCD. Examples of servers and clients within the scope of the invention include financial systems such as the existing ATM networks, stock exchange systems, database systems, security systems, and general purpose computer networks, where the server stores valuable information and a client may be a terminal through which a user can access the server to effectuate desired operations and/or transactions. A large number of servers, clients, and server databases adapted for use with biometric information authentication are known in the art, and all are within the scope of the invention.

The BCD **240** captures biometric information from the user seeking authentication, such as one or more fingerprints, a facial image, voice pattern, image of the retina or iris, etc., and transmits and receives this and other information through the client to and from the server. To enhance the security of the device, the BCD is an integrated hardware apparatus. The device comprises a biometric data acquisition module **242**, a communication module **244**, an encryption module **246**, and a memory **248**. The biometric data acquisition module **242** comprises a biometric sensor and an associated software driver for capturing data. A number of biometric sensors and associated drivers are known in the art, for example video cameras for recording facial images, fingerprint scanners, iris/retinal scanners, and voice recording systems. All are within the scope of the invention. The communication module **244** comprises communication hardware, for example a modem, and associated software, for example a modem driver. The encryption module **246** performs encryption and decryption functions. The encryption and decryption algorithms may be executed by one or more ASICs or by conventional integrated circuits.

Stored in the memory 248 of the BCD is an EK 252 and a serial number BCDN 254, both unique to the BCD. The EK may take the form of any number of encryption keys known in the art, for example a shared symmetric key or the private key of a public key pair. For flexibility, the BCDN and EK can be re-written by an authorized party such as a system administrator or repair technician. Preferably, the BCDN and EK can be rewritten by such external intervention but are readable only by the encryption module. If the BCD is opened by an unauthorized party, the EK and BCDN will be destroyed by erasing them from the memory. This can be achieved by a re-write routine triggered by the opening of the BCD: upon opening, a memory write routine is triggered, causing zeros or random numbers, for example, to be written into the memory locations of the BCDN and EK.

The biometric data acquisition module 242 is preferably designed to ensure that the biometric data is captured live, in real time, as part of the authentication process. This is achieved by verifying the characteristics of a sequence of biometric images as a person allows his or her biometric data to be captured by the biometric sensor. For example, as the person places his or her finger on the scanner, a sequence of images is captured. It has been observed that the captured image changes within the sequence. Because of the elasticity of the finger, the traces of the feature points possess an identifiable characteristic. The variation between the image features of different frames can be calculated to indicate whether the biometric trait has been captured live. For fingerprint capturing, several of the sensors known in the art are designed to detect only fingerprint images captured live. Another example is facial image capturing: as a person approaches a camera, the motion vector variation derived from the facial images has a certain predictable time-varying property. Data which are not captured live, but rather are generated off-line, do not display this time-varying property. Therefore, biometric data captured live will be recognized as different from data which are not.

An example of a user authentication method according to the invention will now be described, with reference to FIG. 3. According to the invention, a user seeking physical or logical access through a client must be the same person whose biometric data is captured by the biometric sensor. The user initiates the authentication process for physical or logical access at a client by entering his or her ID (305). The server, through the client, may prompt the user to input his or her ID. The BCDN may already be known to the client. Alternatively, the server, through the client, may prompt the user to input the BCDN. The server then receives the ID and

BCDN from the client (310).

Subsequently the server, through the client, prompts the user to input live biometric data into the BCD (315). This involves allowing capture of a characteristic image of the user, for example one or more fingerprint images, a facial image, image of the retina or iris, etc. The server then retrieves from the database the EK, which may be any known encryption key, for example a shared symmetric key or the public key of a public key pair, corresponding to the received BCDN (320) and generates a random first RN as a session key or a message identification code (325), which is stored in the server memory. The server encrypts the first RN using the EK (330) and transmits the encrypted first RN to the BCD through the client (335). A time index indicating the time at which the encrypted first RN was transmitted to the BCD is recorded by the server in the server memory or server database for future reference (340).

The BCD receives and decrypts, using the EK resident in the BCD memory, for example a shared symmetric key or the private key of a public key pair, the encrypted first RN (345), captures biometric data (BD) from the user (350), and stores in memory a time index indicating the time at which the BD was captured (355). The BCD then encrypts the BD, the time index, and auxiliary data in an encrypted message using a second RN generated from the first RN as a session key (360). Alternatively, if the first RN is used as a message identification code, the BCD employs the shared symmetric key or the public key of a public key pair corresponding to the server to encrypt the BD, time index, auxiliary data and a second RN generated from the first RN. The BCD then transmits the encrypted message through the client to the server (365). The data items and their order in the encrypted message are preferably pre-defined among the server and all capturing devices linked to the server.

The server receives and decrypts the encrypted message from the BCD (370), using the first session key (retrieved from the server memory) if the first RN is used as a session key, or an encryption key, if the first RN is used as a message identification code. In the latter case, the encryption key may be the shared symmetric key or the private key of the server's public key pair. The server then retrieves previously stored biometric data corresponding to the ID from the database (375). The server then compares the retrieved BD against the BD received from the BCD to determine whether there is a match (380) and calculates the elapsed time between the transmission time index and the capture time index to determine whether a time-out criterion has

been violated (385). If there is a match and if there is no violation of the time-out criterion (390), then the server authenticates the user, who thereby gains physical or logical access as appropriate (395). The server subsequently deletes the first RN (399). Alternatively, if the first RN is used as a message identification code, the server will also compare the second RN (received from the BCD) against the first RN (retrieved from the server memory). Authentication of the user will then occur only if, in addition to the two requirements previously described, the first and second RN also match.

For enhanced security, the server does not keep a record of session keys for future reference. Systematically deleting the session key ensures that the biometric data cannot be decrypted after the time set by the time-out criterion, and that within the time window set by the time-out criterion, only the server can decrypt the biometric data and authenticate the user. Thus, the biometric data is used only once within this very short period. In the case where the RN is used as a message identification code, automatic deletion of the RN assures that the server can not match a RN received from the BCD with a RN retrieved from the server memory after the RN has been used once or after a time interval which may be made as short as is practical given the time delays inherent in information transfer among the various components of the system during a single authentication operation. Thus the biometric data associated with the RN is used only once.

Registration of the BCD must be executed in a very secure way by an authorized individual (registrar), for example a system administrator or technician, who is responsible for certifying the integrity of the entire authentication system. An exemplary registration process may be described as follows: The registrar verifies the structural integrity of the BCD to confirm that it has not been subject to tampering. The registrar then reads the BCDN written on an external surface of the BCD and assigns a unique EK, either a shared symmetric key or a public key pair, to the BCD. The registrar then writes the BCDN and corresponding at least a portion of the EK (shared symmetric key or public key of the public key pair assigned to the BCD) into the sever database and the shared symmetric key or the public key pair into the BCD memory.

Registration of authentication system users may effected by the system administrative staff according to the following exemplary method: The staff assigns a user name or identification number, which may be entirely numeric or alphanumeric in content, to each user.

Live biometric data for each user is then captured using a registered BCD. The biometric data and associated ID are stored in the server database. Subsequently, the staff defines a list of applications, for example physical locations or files of information to which the user is authorized access upon authentication, and stores this information in the server database with the associated ID and biometric data.

The system and method of the invention provide a number of levels of security against fraudulent access. The BCDN and the EK ensure that only registered devices capture the biometric data, *e.g.* a registered fingerprint live-scanner captured the fingerprint image. Live biometric data ensure that only authorized individuals gain access. The request number session key and/or message identification code ensure that only the current message can be used only for the current authentication request. The time-out criterion reduces the time window during which fraudulent access can be attempted.

In an authentication system according to the invention, any authentication request from an open network (that is, without passing through a registered BCD) will be denied. Any authentication request made using static biometric data not captured live will also be denied. Moreover, an encrypted message intercepted during transmission between the BCD and the server cannot be reused because no corresponding request number session key will be found at the server to decrypt the message or no message identification code will be available for verification of the current message.

Various preferred embodiments of the invention have now been described. While these embodiments have been set forth by way of example, various other embodiments and modifications will be apparent to those skilled in the art. Accordingly, it should be understood that the invention is not limited to such embodiments, but encompasses all that which is described in the following claims.

What is claimed is:

1. A method of authenticating biometric data comprising:

encrypting a first session key with a first encryption key;

receiving and decrypting the first session key using a second encryption key;

capturing biometric data (BD) corresponding to a user;

encrypting the captured BD using a second session key;

receiving and decrypting the encrypted captured BD using the first session key;

comparing the captured BD and previously stored BD and verifying that an elapsed time between transmission of the first session key and transmission of the encrypted captured BD does not violate a timeout criterion, so as to authenticate the captured BD; and

destroying the first session key.

2. The method according to claim 1 wherein each of said first and second encryption keys is a shared symmetric key.

3. The method according to claim 1 wherein the first encryption key is a public key of a public key pair and the second encryption key is a private key corresponding to the public key.

4. The method according to claim 1, wherein the first session key is a random number generated by a server.

5. The method according to claim 1 wherein the second session key is generated using the first session key.

6. The method according to claim 1 wherein the first encryption key corresponds to a biometric data capture device serial number (BCDN) unique to a biometric data capture device (BCD).

7. The method according to claim 1 wherein the previously stored BD corresponds to a previously stored user identification code (ID) unique to the user.

8. The method according to claim 1 wherein the first session key is stored in a memory associated with a server and destroyed by deletion from the memory.

9. A method of authenticating biometric data comprising:

encrypting a first message identification code (MIC) with a first encryption key;

receiving and decrypting the first MIC using a second encryption key;

capturing biometric data (BD) corresponding to a user;

encrypting the captured BD and a second MIC using the second encryption key;

receiving and decrypting the encrypted captured BD and second MIC using the first encryption key;

comparing the captured BD and previously stored BD, comparing the second MIC and the first MIC, and verifying that an elapsed time between transmission of the first MIC and transmission of the encrypted captured BD does not violate a timeout criterion, so as to authenticate the captured BD; and

destroying the first MIC.

10. The method according to claim 9 wherein each of the first and second encryption keys is a shared symmetric key.

11. The method according to claim 9, wherein the first MIC is a random number generated by a server wherein said random number corresponds to a biometric data capture device serial number (BCDN).

12. The method according to claim 9 wherein the second MIC is generated using the first MIC.

13. The method according to claim 9 wherein the first encryption key corresponds to a BCDN unique to a biometric data capture device (BCD).

14. The method according to claim 9 wherein the previously stored BD corresponds to a previously stored user identification code (ID) unique to the user.

15. The method according to claim 9 wherein the first MIC is stored in a memory associated with a server and destroyed by deletion from the memory.

16. A method of authenticating biometric data comprising:

encrypting a first message identification code (MIC) with a first at least a portion of a first encryption key;

receiving and decrypting the first MIC using a second at least a portion of the first encryption key;

capturing biometric data (BD) corresponding to a user;

encrypting the captured BD and a second MIC using a first at least a portion of a second encryption key;

receiving and decrypting the encrypted captured BD and second MIC using a second at least a portion of the second encryption key;

comparing the captured BD and previously stored BD, comparing the second MIC and the first MIC, and verifying that an elapsed time between transmission of the first MIC and transmission of the encrypted captured BD does not violate a timeout criterion, so as to authenticate the captured BD; and

destroying the first MIC.

17. The method according to claim 16 wherein each of the first and second encryption keys is a public key pair comprising a public key and a private key corresponding to the public key.

18. The method according to claim 16, wherein the first MIC is a random number generated by a server wherein said random number corresponds to a biometric data capture device serial number (BCDN).

19. The method according to claim 16 wherein the second MIC is generated using the first MIC.

20. The method according to claim 16 wherein the first at least a portion of the first encryption key corresponds to a BCDN unique to a biometric data capture device (BCD).

21. The method according to claim 16 wherein the previously stored BD corresponds to a previously stored user identification code (ID) unique to the user.

22. The method according to claim 16 wherein the first MIC is stored in a memory associated with a server and destroyed by deletion from the memory.

23. A system for authenticating biometric data comprising:

a secure server;

a database connected to said server for storing first biometric data corresponding to a unique ID;

a client connected to said server; and

a biometric data capture device (BCD) connected to said client for capturing second biometric data from a user, said BCD consisting of an integrated hardware unit.

24. The system of claim 23 wherein the server comprises a random number generator.

25. The system according to claim 23 wherein the server comprises a first communication module and a first encryption module.

26. The system according to claim 25 wherein the first communication module comprises a modem and an associated driver for communicating directly with the client and indirectly with the BCD through the client.

27. The system according to claim 25 wherein the first encryption module comprises at least one application specific integrated circuit (ASIC).

28. The system according to claim 23 wherein the database stores a first at least a portion of a first encryption key and a first biometric data capture device serial number (BCDN) corresponding to the first at least a portion of the first encryption key.

29. The system according to claim 23 wherein the integrated hardware unit comprises a biometric data acquisition module, a second communication module, and a second encryption module.

30. The system according to claim 29 wherein the biometric data acquisition module comprises a biometric sensor for capturing a characteristic feature of the user and a sensor driver for acquisition of said second biometric data.

31. The system according to claim 29 wherein the second communication module comprises a modem and an associated driver for communicating directly with the client and indirectly with the server through the client.

32. The system according to claim 29 wherein the second communication module comprises a wireless communication module for communicating directly with the client and indirectly with the server through the client.

33. The system according to claim 29 wherein the second encryption module comprises at least one ASIC.

34. The system according to claim 29 wherein the integrated hardware unit further comprises a memory.

35. The system according to claim 34 wherein the memory stores at separate locations in the memory a unique second BCDN corresponding to the BCD, a unique second at least a portion of the first encryption key corresponding to the BCDN, and a first at least a portion of a second encryption key.

36. The system according to claim 35 wherein the database stores a second at least a portion of the second encryption key.

37. The system according to claim 35 wherein the second BCDN and first and second at least a portion of the first encryption key may be modified by an authorized person.

38. The system according to claim 35 wherein the second BCDN and the second at least a portion of the first encryption key may be read only by the second encryption module.

39. The system according to claim 35 wherein the second BCDN and the second at least a portion of the first encryption key are erased when the BCD is opened by an unauthorized person.

40. The system according to claim 39 wherein the second BCDN and the second at least a portion of the first encryption key are erased by overwriting the separate locations in the memory.

41. The system according to claim 35 wherein each of the first and second encryption keys is a shared symmetric key.

42. The system according to claim 35 wherein each of the first and second encryption keys is a public key pair comprising a public key and a private key corresponding to the private key.

43. The system according to claim 23 wherein the server comprises a server memory.

44. A system for authenticating biometric data for controlling physical and/or logical access comprising:

a secure server comprising a random number generator, a first communication module, a

first encryption module, and a server memory;

a database connected to said server for storing a first at least a portion of each of first and second encryption keys, a first biometric data capture device serial number (BCDN) corresponding to the at least a portion of the first encryption key, a unique user identification code (ID) corresponding to a user, and first biometric data corresponding to said ID;

a client connected to said server; and

a biometric data capture device (BCD) connected to said client for capturing second biometric data from a user, said BCD consisting of an integrated hardware unit comprising a biometric data acquisition module, a second communication module, a second encryption module, and a BCD memory, said BCD being associated with a unique second BCDN stored in said BCD memory and a second at least a portion of the first encryption key stored in said BCD memory.

45. A method of verifying live capture of biometric data comprising:

capturing a sequence of characteristic feature inputs by a user;

extracting from the sequence a time-varying property of the characteristic feature inputs wherein said time-varying property is known to evolve in a predictable manner; and

comparing the evolution of the time-varying property against a predictive model.

46. A biometric data capture device for verifying live capture of biometric data comprising:

a biometric sensor for capturing a characteristic feature of a user;

a sensor driver for acquiring biometric data corresponding to the user; and

means for verifying live capture of the biometric data.

47. A method of authenticating biometric data comprising:

encrypting a first session key with a first encryption key;

receiving and decrypting the first session key using a second encryption key;

capturing biometric data (BD) corresponding to a user;

capturing a sequence of characteristic feature inputs by the user;

extracting from the sequence a time-varying property of the characteristic feature inputs wherein the time-varying property is known to evolve in a predictable manner; and

comparing the evolution of the time-varying property against a predictive model.

encrypting the captured BD using a second session key;

receiving and decrypting the encrypted captured BD using the first session key;

comparing the captured BD and previously stored BD, verifying that the evolution of the time varying property matches a predictive model, and verifying that an elapsed time between transmission of the first session key and transmission of the encrypted captured BD does not violate a timeout criterion, so as to authenticate the captured BD; and

destroying the first session key.

48. The method according to claim 47 wherein each of said first and second encryption keys is a shared symmetric key.

49. The method according to claim 47 wherein the first encryption key is a public key of a public key pair and the second encryption key is a private key corresponding to the public key.

50. The method according to claim 47, wherein the first session key is a random number generated by a server.

51. The method according to claim 47 wherein the second session key is generated using the first session key.

52. The method according to claim 47 wherein the first encryption key corresponds to a biometric data capture device serial number (BCDN) unique to a biometric data capture device (BCD).

53. The method according to claim 47 wherein the previously stored BD corresponds to a previously stored user identification code (ID) unique to the user.

54. The method according to claim 47 wherein the first session key is stored in a memory associated with a server and destroyed by deletion from the memory.

55. A method of authenticating biometric data comprising:

encrypting a first message identification code (MIC) with a first encryption key;

receiving and decrypting the first MIC using a second encryption key;

capturing biometric data (BD) corresponding to a user;

capturing a sequence of characteristic feature inputs by the user;

extracting from the sequence a time-varying property of the characteristic feature inputs wherein the time-varying property is known to evolve in a predictable manner; and

comparing the evolution of the time-varying property against a predictive model.

encrypting the captured BD and a second MIC using the second encryption key;

receiving and decrypting the encrypted captured BD and second MIC using the first encryption key;

comparing the captured BD and previously stored BD, comparing the second MIC and the first MIC, verifying that the evolution of the time varying property matches a predictive model, and verifying that an elapsed time between transmission of the first MIC and transmission of the encrypted captured BD does not violate a timeout criterion, so as to authenticate the captured BD; and

destroying the first MIC.

56. The method according to claim 55 wherein each of the first and second encryption keys is a shared symmetric key.

57. The method according to claim 55, wherein the first MIC is a random number generated by a server wherein said random number corresponds to a biometric data capture device serial number (BCDN).

58. The method according to claim 55 wherein the second MIC is generated using the first MIC.

59. The method according to claim 55 wherein the first encryption key corresponds to a BCDN unique to a biometric data capture device (BCD).

60. The method according to claim 55 wherein the previously stored BD corresponds to a previously stored user identification code (ID) unique to the user.

61. The method according to claim 55 wherein the first MIC is stored in a memory associated

with a server and destroyed by deletion from the memory.

62. A method of authenticating biometric data comprising:

encrypting a first message identification code (MIC) with a first at least a portion of a first encryption key;

receiving and decrypting the first MIC using a second at least a portion of the first encryption key;

capturing biometric data (BD) corresponding to a user;

capturing a sequence of characteristic feature inputs by the user;

extracting from the sequence a time-varying property of the characteristic feature inputs wherein the time-varying property is known to evolve in a predictable manner; and

comparing the evolution of the time-varying property against a predictive model.

encrypting the captured BD and a second MIC using a first at least a portion of a second encryption key;

receiving and decrypting the encrypted captured BD and second MIC using a second at least a portion of the second encryption key;

comparing the captured BD and previously stored BD, verifying that the evolution of the time varying property matches a predictive model, comparing the second MIC and the first MIC, and verifying that an elapsed time between transmission of the first MIC and transmission of the encrypted captured BD does not violate a timeout criterion, so as to authenticate the captured BD; and

destroying the first MIC.

63. The method according to claim 62 wherein each of the first and second encryption keys is a public key pair comprising a public key and a private key corresponding to the public key.

64. The method according to claim 62, wherein the first MIC is a random number generated by a server wherein said random number corresponds to a biometric data capture device serial number (BCDN).

65. The method according to claim 62 wherein the second MIC is generated using the first

MIC.

66. The method according to claim 62 wherein the first at least a portion of the first encryption key corresponds to a BCDN unique to a biometric data capture device (BCD).

67. The method according to claim 62 wherein the previously stored BD corresponds to a previously stored user identification code (ID) unique to the user.

68. The method according to claim 62 wherein the first MIC is stored in a memory associated with a server and destroyed by deletion from the memory.

69. A system for authenticating biometric data comprising:

a secure server;

a database connected to said server for storing first biometric data corresponding to a unique user identification code (ID);

a client connected to said server; and

a biometric data capture device (BCD) connected to said client for capturing second biometric data from a user, said BCD consisting of an integrated hardware unit comprising means for verifying live capture of the second BD.

70. The system of claim 69 wherein the server comprises a random number generator.

71. The system according to claim 69 wherein the server comprises a first communication module and a first encryption module.

72. The system according to claim 71 wherein the first communication module comprises a modem and an associated driver for communicating directly with the client and indirectly with the BCD through the client.

73. The system according to claim 71 wherein the first encryption module comprises at least one application specific integrated circuit (ASIC).

74. The system according to claim 69 wherein the database stores a first at least a portion of a first encryption key and a first biometric data capture device serial number (BCDN) corresponding to the first at least a portion of the first encryption key.

75. The system according to claim 69 wherein the integrated hardware unit further comprises a

biometric data acquisition module, a second communication module, and a second encryption module.

76. The system according to claim 75 wherein the biometric data acquisition module comprises a biometric sensor for capturing a characteristic feature of the user and a sensor driver for acquisition of said second biometric data.

77. The system according to claim 75 wherein the second communication module comprises a modem and an associated driver for communicating directly with the client and indirectly with the server through the client.

78. The system according to claim 75 wherein the second communication module comprises a wireless communication module for communicating directly with the client and indirectly with the server through the client.

79. The system according to claim 75 wherein the second encryption module comprises at least one ASIC.

80. The system according to claim 75 wherein the integrated hardware unit further comprises a memory.

81. The system according to claim 80 wherein the memory stores at separate locations in the memory a unique second BCDN corresponding to the BCD, a unique second at least a portion of the first encryption key corresponding to the BCDN, and a first at least a portion of a second encryption key.

82. The system according to claim 81 wherein the database stores a second at least a portion of the second encryption key.

83. The system according to claim 81 wherein the second BCDN and first and second at least a portion of the first encryption key may be modified by an authorized person.

84. The system according to claim 81 wherein the second BCDN and the second at least a portion of the first encryption key may be read only by the second encryption module.

85. The system according to claim 81 wherein the second BCDN and the second at least a portion of the first encryption key are erased when the BCD is opened by an unauthorized person.

86. The system according to claim 85 wherein the second BCDN and the second at least a portion of the first encryption key are erased by overwriting the separate locations in the memory.

87. The system according to claim 81 wherein each of the first and second encryption keys is a shared symmetric key.

88. The system according to claim 81 wherein each of the first and second encryption keys is a public key pair comprising a public key and a private key corresponding to the private key.

89. The system according to claim 69 wherein the server comprises a server memory.

90. A method of registering a biometric data capture device (BCD) comprising:

assigning a first encryption key to the BCD;

writing a first at least a portion of the first encryption key and a biometric data capture device serial number (BCDN) corresponding to the BCD into a database; and

writing a second at least a portion of the first encryption key, a first at least a portion of a second encryption key, and the BCDN into a memory internal to the BCD.

91. The method according to claim 90 further comprising inspecting the BCD to determine if it has been subject to tampering.

92. The method according to claim 90 further comprising reading the BCDN from the BCD.

93. The method according to claim 90 wherein each of the first and second encryption keys is a shared symmetric key.

94. The method according to claim 90 wherein each of the first and second encryption keys is a public key pair comprising a public key and a private key corresponding to the public key.

95. A method of registering a user of an authentication system comprising:

assigning a user identification code (ID) to the user;

capturing live biometric data for the user;

storing the biometric data and associated ID in a database; and

defining a list of applications to which the user is authorized access.

96. The method according to claim 95 further comprising storing the list in the database.

97. The method according to claim 95 wherein the list is associated with the ID and the captured live biometric data.

98. A method or preventing re-use of biometric data comprising:

generating a first session key;

using the first session key to decrypt encrypted captured biometric data; and

destroying the first session key.

99. The method according to claim 98 further comprising encrypting the captured biometric data using a second session key.

100. The method according to claim 99 wherein the second session key is generated using the first session key.

101. The method according to claim 99 wherein each of the first and second session keys is a random number.

102. The method according to claim 98 further comprising encrypting the first session key with a first encryption key.

103. The method according to claim 102 wherein the first encryption key corresponds to a biometric data capture device serial number (BCDN).

104. The method according to claim 102 further comprising decrypting the encrypted first session key with a second encryption key.

105. The method according to claim 104 wherein each of the first and second encryption keys is a shared symmetric key.

106. The method according to claim 104 wherein the first encryption key is a public key of a public key pair and the second encryption key is a private key corresponding to the public key.

107. The method according to claim 102 further comprising comparing the captured biometric data to previously stored biometric data.

108. The method according to claim 107 further comprising verifying that an elapsed time between a transmission of the first session key and a transmission of the encrypted captured

biometric data does not violate a time-out criterion.

109. A method or preventing re-use of biometric data comprising:

generating a first message identification code (MIC);

decrypting encrypted captured biometric data and a second MIC; and

destroying the first MIC.

110. The method according to claim 109 further comprising encrypting the first MIC with a first at least a portion of a first encryption key.

111. The method according to claim 110 further comprising decrypting the encrypted first MIC with a second at least a portion of the first encryption key.

112. The method according to claim 111 further comprising encrypting the captured biometric data and the second MIC using a first at least a portion of a second encryption key.

113. The method according to claim 112 further comprising decrypting the encrypted captured biometric data and second MIC using a second at least a portion of the second encryption key.

114. The method according to claim 113 wherein the first at least a portion of the first encryption key corresponds to a biometric data capture device serial number (BCDN).

115. The method according to claim 113 wherein each of the first and second encryption keys is a shared symmetric key.

116. The method according to claim 113 wherein each of the first and second encryption keys is a public key pair comprising a public key and a private key corresponding to the public key.

117. The method according to claim 113 further comprising comparing the captured biometric data to previously stored biometric data and the first MIC to the second MIC.

118. The method according to claim 117 further comprising verifying that an elapsed time between transmission of the first MIC and transmission of the encrypted captured biometric data does not violate a time-out criterion.

119. The method according to claim 109 wherein the second MIC is generated using the first MIC.

120. The method according to claim 109 wherein each of the first and second MIC is a random number.

DRAWINGS

FIGURE 1. PRIOR ART

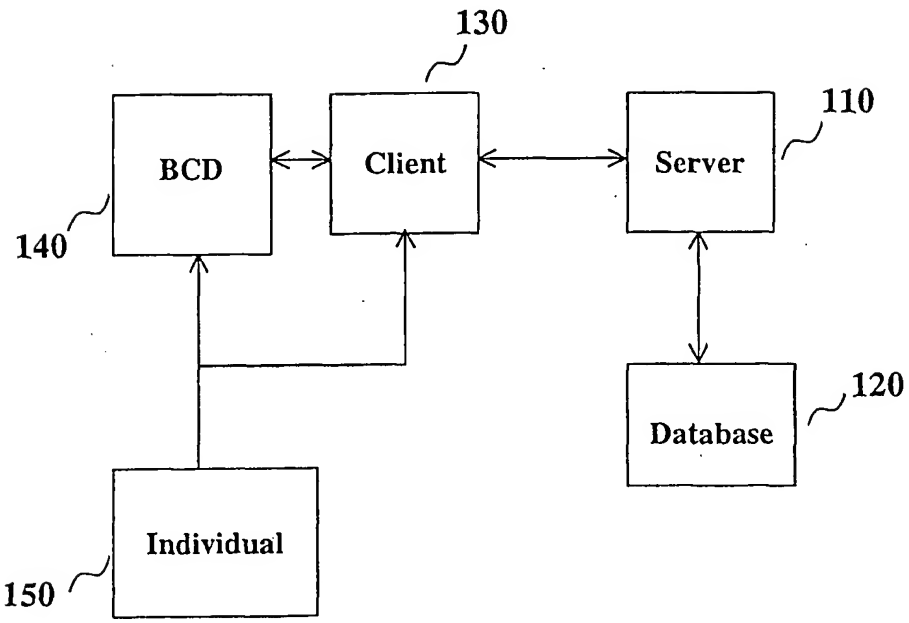


FIGURE 2

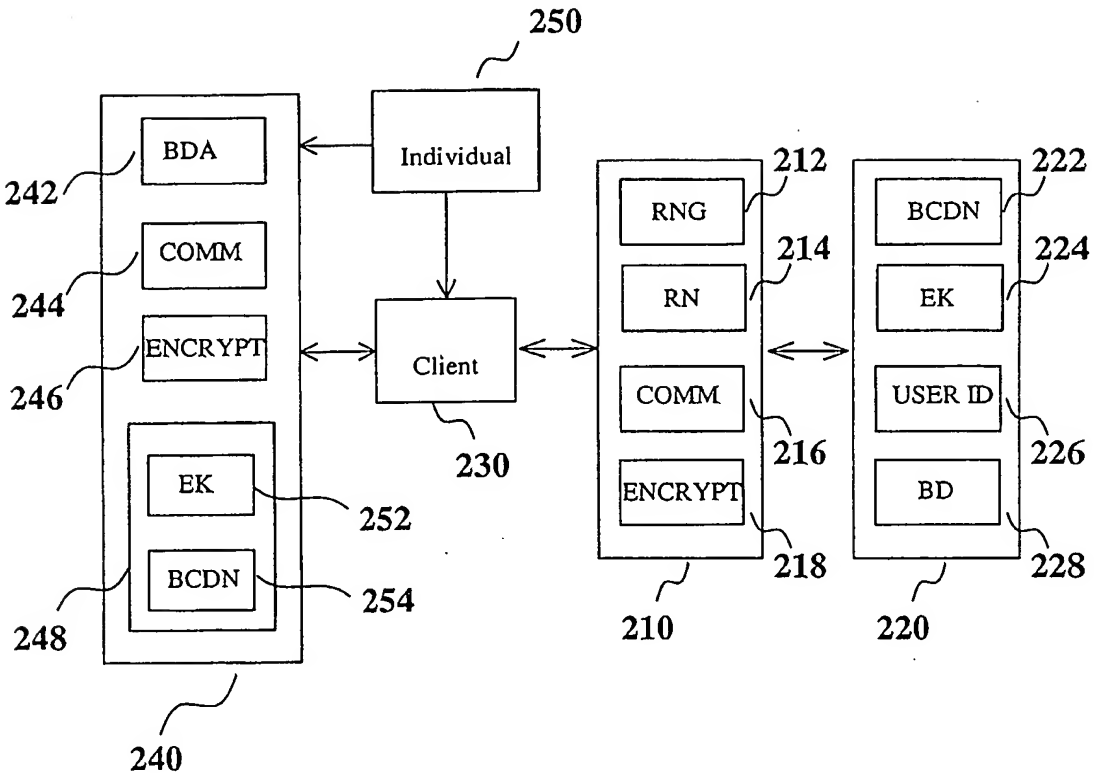
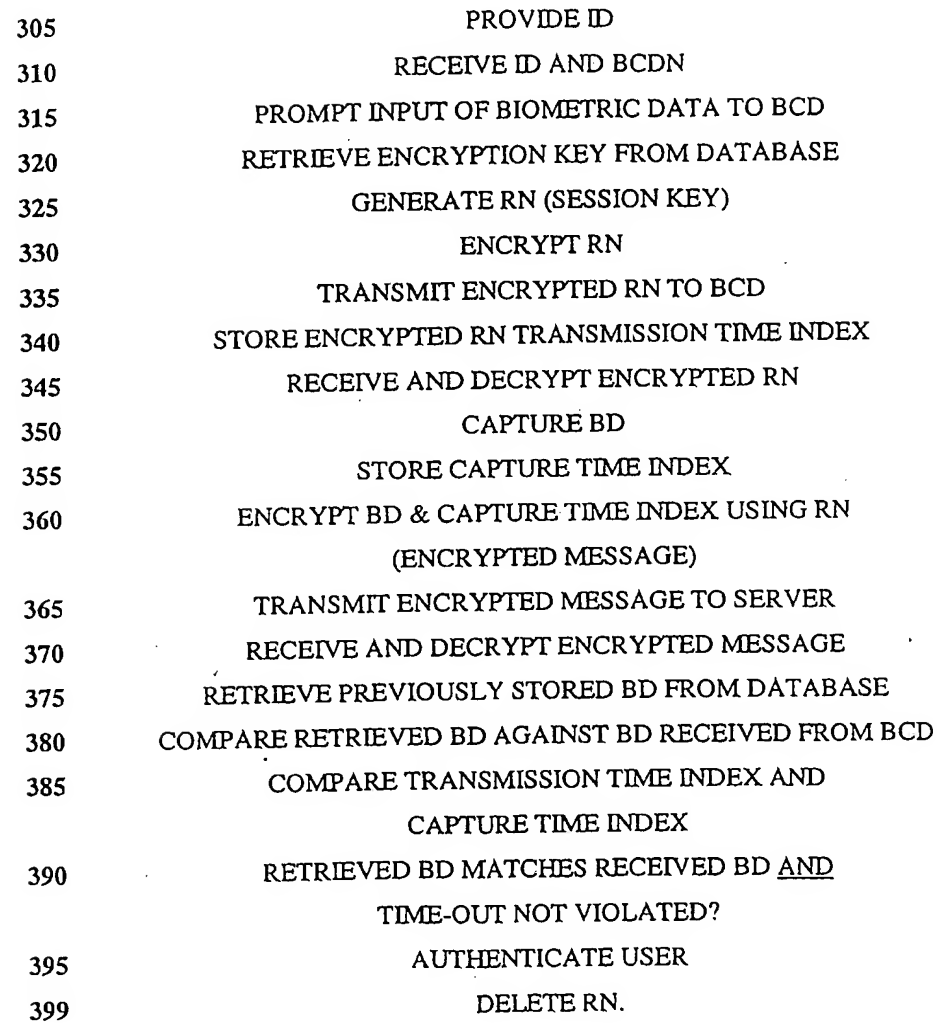

250
Individual
BDA
242
COMM
244
ENCRYPT
246
Client
230
EK
252
BCDN
254
248
240
RNG
212
RN
214
COMM
216
ENCRYPT
218
210
BCDN
222
EK
224
USER ID
226
BD
228
220

FIGURE 3


305
PROVIDE ID
310
RECEIVE ID AND BCDN
315
PROMPT INPUT OF BIOMETRIC DATA TO BCD
320
RETRIEVE ENCRYPTION KEY FROM DATABASE
325
GENERATE RN (SESSION KEY)
330
ENCRYPT RN
335
TRANSMIT ENCRYPTED RN TO BCD
340
STORE ENCRYPTED RN TRANSMISSION TIME INDEX
345
RECEIVE AND DECRYPT ENCRYPTED RN
350
CAPTURE BD
355
STORE CAPTURE TIME INDEX
360
ENCRYPT BD & CAPTURE TIME INDEX USING RN
(ENCRYPTED MESSAGE)
365
TRANSMIT ENCRYPTED MESSAGE TO SERVER
370
RECEIVE AND DECRYPT ENCRYPTED MESSAGE
375
RETRIEVE PREVIOUSLY STORED BD FROM DATABASE
380
COMPARE RETRIEVED BD AGAINST BD RECEIVED FROM BCD
385
COMPARE TRANSMISSION TIME INDEX AND
CAPTURE TIME INDEX
390
RETRIEVED BD MATCHES RECEIVED BD AND
TIME-OUT NOT VIOLATED?
395
AUTHENTICATE USER
399
DELETE RN.

INTERNATIONAL SEARCH REPORT

Internatio cation No.
PCT/SG 00/00177

CLASSIFICATION OF SUBJECT MATTER

IPC[7]: A61B 5/117, G06F 1/00, H04B 1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7]: A61B, G06F, H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5229764 A (MATCHETT) 20 July 1993 (20.07.93) *abstract, col.1, l.1-11; col.1, l.60 - col.2, l.3; col. 3, l. 10-44; col. 6, l. 8-48; col. 8, l. 48-67.*	23-25,32,34, 46, 69
A		26-31,44,70-89
A	US 6076167 A (BORZA) 13 June 2000 (13.06.00) *abstract; fig. 5.*	1,47

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
„A" document defining the general state of the art which is not considered to be of particular relevance
„E" earlier application or patent but published on or after the international filing date
„L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
„O" document referring to an oral disclosure, use, exhibition or other means
„P" document published prior to the international filing date but later than the priority date claimed
„T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
„X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
„Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 February 2002 (19.02.2002)	28 February 2002 (28.02.2002)
Name and mailing adress of the ISA/AT Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna Facsimile No. 1/53424/535	Authorized officer ZAWODSKY Telephone No. 1/53424/346

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte al application No.
PCT/SG 00/00177

Patent document cited in search report			Publication date	Patent family member(s)			Publication date
US	A	5229764	20-07-1993			none	
US	A	6078167	13-06-2000	AU	A1	52185/98	29-06-1998
				EP	A1	944980	29-09-1999
				WO	A1	9825385	11-06-1998